Council of the European Union
General Secretariat

Brussels, 19 October 2021

Interinstitutional files:
2020/0361 (COD)

WK 12468/2021 INIT

LIMITE

COMPET	**PI**
MI	**AUDIO**
JAI	**CONSOM**
TELECOM	**CODEC**
CT	**JUSTCIV**

This is a paper intended for a specific community of recipients. Handling and further distribution are under the sole responsibility of community members.

NOTE

From:	NL Delegation
To:	Delegations
Subject:	Digital Services Act: NL comments on the 2nd compromise text

MEMBER STATE	The Netherlands (hereinafter NL)	NL
GENERAL COMMENTS:		
COMMISSION PROPOSAL	**Drafting suggestions**	**Comments**
2020/0361 (COD)		
Proposal for a **REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on a Single Market For Digital Services (Digital Services Act) and amending Directive 2000/31/EC**		
(Text with EEA relevance)		
THE EUROPEAN PARLIAMENT AND THE COUNCIL OF THE EUROPEAN UNION,		
Having regard to the Treaty on the Functioning of the European Union, and in particular Article 114 thereof,		
Having regard to the proposal from the European Commission,		
After transmission of the draft legislative act to the national parliaments,		

MEMBER STATE	The Netherlands (hereinafter NL)	NL
GENERAL COMMENTS:		
COMMISSION PROPOSAL	**Drafting suggestions**	**Comments**
Having regard to the opinion of the European Economic and Social Committee[1],		
[Having regard to the opinion of the Committee of the Regions[2],**]**		
~~Having regard to the opinion of the European Data Protection Supervisor[3],~~		
Acting in accordance with the ordinary legislative procedure,		
Whereas:		
LIMITED LIABILITY EXEMPTION CLARIFICATION		
(20) A provider of intermediary services that deliberately collaborates with a	(20) A provider of intermediary services that deliberately collaborates with a recipient of the services in order to undertake illegal activities does not provide its service	*Many hosting providers take measures to tackle illegal content online, making it harder for criminals to develop illegal activities online. At the same time, there are providers filling this gap by making it their business model to*

1 OJ C , , p. .

2 OJ C , , p. .

3 ~~OJ C, p.~~

MEMBER STATE	The Netherlands (hereinafter NL)	NL
GENERAL COMMENTS:		
COMMISSION PROPOSAL	**Drafting suggestions**	**Comments**
recipient of the services in order to undertake illegal activities does not provide its service neutrally and should therefore not be able to benefit from the exemptions from liability provided for in this Regulation. **This is the case, in particular, where it provides its service with the main purpose of facilitating illegal activities. The fact alone that a service offers encrypted transmissions should not in itself qualify as deliberate collaboration.**	neutrally and should therefore not be able to benefit from the exemptions from liability provided for in this Regulation. **This is the case, in particular, where it provides its service with the main purpose of facilitating illegal activities. The fact alone that a service offers encrypted transmissions should not in itself qualify as deliberate collaboration.** ***When determining if this is the case the following circumstances can be taken into account which, alone or in conjunction, can indicate that a provider of intermediary services does not provide its service neutrally: the services are hosted on the 'dark web', a large part of the information or activities that its recipients provide or undertake is illegal, the provider of intermediary services provides an unusually high level of anonymity to recipients, the provider offers its services to recipients that indicate they intend to use the services to render illegal activities, the provider provides advice to recipients on how to prevent authorities from intervening with their activities, e.g. by advising in which jurisdiction the recipient can best store certain information, the provider advertises itself or its services to potential recipients as being willing to facilitate***	*offer crime as a service. As such, they intentionally and deliberately facilitate illegal activities such as the dissemination of child pornography, the trading in illegal goods, such as weapons, drugs, human trafficking and allowing cyber-attacks. By intentionally offering crime as a service, these providers could not be said to be 'neutral'. These so called 'bad hosts' or 'bulletproof hosts' should therefore not be able to benefit from the exemptions for liability offered in the DSA. The text proposal is aimed at clarifying this.*

MEMBER STATE	The Netherlands (hereinafter NL)	NL
GENERAL COMMENTS:		
COMMISSION PROPOSAL	**Drafting suggestions**	**Comments**
	criminal activities and that its services are suited for that purpose.	
GENERAL – SPECIFIC MONITORING		
(28) Providers of intermediary services should not be subject to a monitoring obligation with respect to obligations of a general nature. This does not concern monitoring obligations in a specific case and, in particular, does not affect orders by national authorities in accordance with national legislation, in accordance with the conditions established in this Regulation. **Such orders should not consist in requiring a service provider to introduce, exclusively at its own expense, a screening system which entails general and permanent monitoring in order to prevent any future infringement. However, such orders may require a provider of hosting services to remove information which it stores, the content of which is identical or equivalent to the content of information which was previously declared to be unlawful, or to block access to that information, irrespective of who requested the storage of that information, provided that the monitoring of and search for the information concerned is**	(28) Providers of intermediary services should not be subject to a monitoring obligation with respect to obligations of a general nature. This does not concern monitoring obligations in a specific case***. The ban on a general monitoring obligation on intermediary services should not prevent Member States from imposing monitoring obligations of a specific nature, provided, they meet the principles of proportionality and necessity, are in conformity with the conditions as set out by any relevant Union law, including CJEU case-law, and the illegal content in question is specific, well-defined and delineated. A monitoring obligation that requires providers of intermediary services to perform a general search of all content in order to find any potential illegal content, imposes an obligation that requires a provider to carry out an independent assessment or goes ~~an specific monitoring obligation that puts excessive burdens or requires unreasonable or excessive resources and measures by intermediary~~***	Following the most recent Internal Market Council Working Party of 14 October, during which Chapters I & II including Recital 28 were discussed, we noticed some delegations had expressed their concerns about the phrase relating to "excessive burdens" and claimed it to be out of line with the CJEU's judgment in *Glawischnig-Piesczek v Facebook Ireland Limited*. To allay their concerns, we have provided for the text highlighted in yellow, which we believe neatly dovetails with paragraphs 45 and 46 of the CJEU's ruling. For ease of reference, we have copied the relevant wording the Court used below: 44 Thus, Article 15(1) of Directive 2000/31 implies that the objective of an injunction such as the one referred to in Article 18(1) of that directive, read in conjunction with recital 41, consisting, inter alia, of effectively protecting a person's reputation and honour, may not be pursued by imposing an excessive obligation on the host provider.

MEMBER STATE	The Netherlands (hereinafter NL)	NL
GENERAL COMMENTS:		
COMMISSION PROPOSAL	**Drafting suggestions**	**Comments**
limited to information properly identified in the injunction, such as the name of the person concerned by the infringement determined previously, the circumstances in which that infringement was determined and equivalent content to that which was declared to be illegal, and does not require the provider of hosting services to carry out an independent assessment of that content. Nothing in this Regulation should be construed as an imposition of a general monitoring obligation or **a general** active fact-finding obligation, or as a general obligation for providers to take proactive measures to relation to illegal content.	***~~services~~ beyond the use of readily-available automated tools and technologies, should be considered a general monitoring obligation. It follows from relevant CJEU case-law that specific monitoring obligations may be accompanied by a corollary responsibility on intermediary services to remove (access to), or block identical to, or essentially equivalent, content which it stores, that has previously been declared to be illegal or unlawful, as specified in the specific monitoring obligation, insofar this does not compel intermediary to carry out an independent assessment of that specific content. ~~and~~*** **,** In particular**~~,~~** ***it*** does not affect orders by national authorities in accordance with national legislation, in accordance with the conditions established in this Regulation. **Such orders should not consist in requiring a service provider to introduce, exclusively at its own expense, a screening system which entails general and permanent monitoring in order to prevent any future infringement. However, such orders may require a provider of hosting services to remove information which it stores, the content of which is identical or equivalent to the content of information which was previously declared to be**	45 In light of the foregoing, it is important that the equivalent information referred to in paragraph 41 above contains specific elements which are properly identified in the injunction, such as the name of the person concerned by the infringement determined previously, the circumstances in which that infringement was determined and equivalent content to that which was declared to be illegal. Differences in the wording of that equivalent content, compared with the content which was declared to be illegal, must not, in any event, be such as to require the host provider concerned to carry out an independent assessment of that content. 46 In those circumstances, an obligation such as the one described in paragraphs 41 and 45 above, on the one hand — in so far as it also extends to information with equivalent content — appears to be sufficiently effective for ensuring that the person targeted by the defamatory statements is protected. On the other hand, that protection is not provided by means of an excessive obligation being imposed on the host provider, in so far as the monitoring of and search for information which it requires are limited to information containing the elements specified in the injunction, and its defamatory content of an equivalent nature does not require the

MEMBER STATE	The Netherlands (hereinafter NL)	NL
GENERAL COMMENTS:		
COMMISSION PROPOSAL	**Drafting suggestions**	**Comments**
	unlawful, or to block access to that information, irrespective of who requested the storage of that information, provided that the monitoring of and search for the information concerned is limited to information properly identified in the injunction, such as the name of the person concerned by the infringement determined previously, the circumstances in which that infringement was determined and equivalent content to that which was declared to be illegal, and does not require the provider of hosting services to carry out an independent assessment of that content. Nothing in this Regulation should be construed as an imposition of a general monitoring obligation or **a general** active fact-finding obligation, or as a general obligation for providers to take proactive measures to relation to illegal content.	host provider to carry out an independent assessment, since the latter has recourse to automated search tools and technologies. 47 Thus, such an injunction specifically does not impose on the host provider an obligation to monitor generally the information which it stores, or a general obligation actively to seek facts or circumstances indicating illegal activity, as provided for in Article 15(1) of Directive 2000/31.
ADDRESSING THE ISSUE OF ABUSE OF HOSTING FOR MANIFESTLY CRIMINAL OFFENCES		
No original text	**(42b)** ***Article [15b] requires providers of hosting services [that are not online platforms] to take basic measures in order to address the risk of misuse of their services for manifestly criminal offences and to mitigate such offences if any actual misuse occurs. Examples of manifestly***	Please refer to NEW Article 15b, which this new Recital pertains to. The 'place' for this new Recital, i.e. 42b, is merely a suggestion; we wished to stay as close as possible to the Article build-up and numerical order of the DSA and the corresponding recitals, but remain open for a more appropriate order if necessary.

MEMBER STATE	The Netherlands (hereinafter NL)	NL
GENERAL COMMENTS:		
COMMISSION PROPOSAL	Drafting suggestions	Comments
	criminal activities are the dissemination of CSAM, malware (including ransomware) and phishing emails, and the hosting of malicious or fraudulent webshops. Public and private information resources are often available to inform hosting providers of known software vulnerabilities, threats, abuse and cybercrime incidents. Examples are Computer Emergency Response Teams (CERTs) and available abuse feeds. Providers of hosting services should connect to these information sources to obtain this information. In some countries, such information can also be shared with providers of hosting services without prior request. Providers of hosting services should have procedures and technical measures in place which enables them to process this information adequately, and act accordingly if needed. These measures should be carried out in a reasonable, proportionate, effective and non-discriminatory way.	

MEMBER STATE	The Netherlands (hereinafter NL)	NL
GENERAL COMMENTS:		
COMMISSION PROPOSAL	Drafting suggestions	Comments
Chapter III **Due diligence obligations for a transparent and safe online environment**		
SECTION 2 **ADDITIONAL PROVISIONS APPLICABLE TO PROVIDERS OF HOSTING SERVICES, INCLUDING ONLINE PLATFORMS**		

NO ORIGINAL TEXT	*NEW Article 15b* *Measures and protection against misuse* ***Providers of hosting services [that are not online platforms] shall:*** ***1. ensure that paying users can only use its services when the provider has obtained the name, address, telephone number, electronic mail address and bank account details of the user. Art. 22.2 – 22.5 are applicable;*** ***2. connect to available information sources to obtain, or be able to receive, and adequately process information on manifestly criminal offences and vulnerabilities regarding their networks and the type of service they provide;*** ***3. take immediate measures to prevent further harm when knowledge is obtained about manifestly criminal offences being committed through the use of its services and the continuation of those manifestly criminal offences may result in serious harm;*** ***4. promptly inform recipients of the services when knowledge is obtained about manifestly criminal offences being committed through or by***	After having circulated our original amendment in the Internal Market Working Party and other relevant Council configurations, it became apparent that whilst some could support our text, there was no majority for our suggestions. To this end, we have drafted an alternative text which we believe could be more amenable to a majority of the Member States. To support a fruitful and open discussion, we have set out an alternative below which provides for concrete, specific obligations, commensurate with the concrete nature of clear-cut due diligence obligations incumbent on online intermediaries that fall within the scope of the DSA. In addition, we have drafted an accompanying recital (please refer to the text below NEW Article 15b and new Recital (42b) above) that further elucidates the workings of this provision. The original proposal also raised the question as to whether the measures should apply to all hosting providers, or only hosting providers that are not online platforms. Finally, we aim to exclusively target users that "pay" for the use of hosting services by pecuniary means, whichever form and/or shape this may take, e.g. regular or virtual currencies. We do not intend to capture those users who use "free" services, e.g. registering for a Gmail account for private correspondence use. However, given that we are unsure about which term may be most appropriate in EU law to delineate such users, we would like to call on, and be greatly appreciative of, the European Commission's and Council legal services' help in this regard.

MEMBER STATE	The Netherlands (hereinafter NL)	NL
GENERAL COMMENTS:		
COMMISSION PROPOSAL	Drafting suggestions	Comments
	those recipients, or when knowledge is obtained about serious vulnerabilities in hardware or software that can be abused for such offences; *5.* *(a) suspend, for a reasonable period of time and after having issued a prior warning, the provision of their services to recipients of the service that frequently provide manifestly criminal content or commit manifestly criminal offences;* *(b) assess, on a case-by-case basis and in a timely, diligent and objective manner, whether a recipient, individual or entity engages in the misuse referred to in paragraph 5, sub (a), taking into account all relevant facts and circumstances apparent from the information available to the provider. Those circumstances shall include at least the following:* *i. the absolute numbers of items of manifestly criminal content or manifestly criminal offences, submitted in the past year;*	We hope to have an open discussion on this issue, including on the question whether to limit the scope to providers of hosting services that are not online platforms, or to also apply our suggestions to online platforms.

MEMBER STATE	The Netherlands (hereinafter NL)	NL
GENERAL COMMENTS:		
COMMISSION PROPOSAL	Drafting suggestions	Comments
	ii. the relative proportion thereof in relation to the total number of items of information provided in the past year; *iii. the gravity of the misuses and its consequences;* *iv. the intention of the recipient, individual or entity.* *(c) set out, in a clear and detailed manner, their policy in respect of the in their terms and conditions, including as regards the facts and circumstances that they take into account when assessing whether certain behaviour constitutes misuse, and the duration of the suspension.* *Accompanying Recital 42(b):* *Article [15b] requires providers of hosting services [that are not online platforms] to take basic measures in order to address the risk of misuse of their services for manifestly criminal offences and to mitigate such offences if any actual misuse occurs. Examples of manifestly criminal activities are the dissemination of CSAM, malware (including ransomware) and phishing emails, and the hosting of*	

MEMBER STATE	The Netherlands (hereinafter NL)	NL
GENERAL COMMENTS:		
COMMISSION PROPOSAL	Drafting suggestions	Comments
	malicious or fraudulent webshops. Public and private information resources are often available to inform hosting providers of known software vulnerabilities, threats, abuse and cybercrime incidents. Examples are Computer Emergency Response Teams (CERTs) and available abuse feeds. Providers of hosting services should connect to these information sources to obtain this information. In some countries, such information can also be shared with providers of hosting services without prior request. Providers of hosting services should have procedures and technical measures in place which enables them to process this information adequately, and act accordingly if needed. These measures should be carried out in a reasonable, proportionate, effective and non-discriminatory way.	
NOTICE & ACTION (N&A) MECHANISM		

Article 14 *Notice and action mechanisms*	*Article 14* *Notice and action mechanisms*	*NL believes that requiring individuals to list their name jeopardizes users' anonymity on the Internet, which, in turn, could undermine the fundamental right to privacy, freedom of expression and freedom of information online.* *Additionally, shame or fear of retaliation may create a disincentive for victims and other notifiers from flagging the illegal content in question.* *Anonymous notices should therefore be the norm unless there is a justified exception and should have the same legal effect as non-anonymous notices, i.e. give rise to actual knowledge pursuant to Article 14(3) of the DSA proposal. For instance when the entity submitting the notice argues that certain information is protected by trademark law and he or she is the trademark owner.* *Given the lack of support for our amendment during the first written round in July, however, we would like to express our support for Germany's amendment under Article 14.2(c).* *With respect to paragraph 1, we can subscribe to Germany's proposals to facilitate access to the notice & action mechanism for individual users or entities by providing mechanisms in the language of every Member State in which the provider operates.*
1. Providers of hosting services shall put mechanisms in place to allow any individual or entity to notify them of the presence on their service of specific items of information that the individual or entity considers to be illegal content. Those mechanisms shall be easy to access, user-friendly, and allow for the submission of notices exclusively by electronic means.	1. Providers of hosting services shall put mechanisms in place to allow any individual or entity to notify them of the presence on their service of specific items of information that the individual or entity considers to be illegal content. Those mechanisms shall be easy to access, user-friendly, and allow for the submission of notices exclusively by electronic means ***and in the language of every Member State in which the provider operates***.	
2. The mechanisms referred to in paragraph 1 shall be such as to facilitate the submission of sufficiently precise and adequately substantiated notices, ~~on the basis of which a diligent economic operator can identify the illegality of the content in question~~. To that	2. The mechanisms referred to in paragraph 1 shall be such as to facilitate the submission of sufficiently precise and adequately substantiated notices, ~~on the basis~~	

MEMBER STATE	The Netherlands (hereinafter NL)	NL
GENERAL COMMENTS:		
COMMISSION PROPOSAL	Drafting suggestions	Comments
end, the providers shall take the necessary measures to enable and facilitate the submission of notices containing all of the following elements: (a) a~~n~~ **sufficiently substantiated** explanation of the reasons why the individual or entity considers the information in question to be illegal content; (b) a clear indication of the electronic location of that information, ~~in particular~~**such as** the exact URL or URLs, and, where necessary, additional information enabling the identification of the illegal content;	~~of which a diligent economic operator can identify the illegality of the content in question~~. To that end, the providers shall take the necessary measures to enable and facilitate the submission of notices containing all of the following elements: (a) a~~n~~ **sufficiently substantiated** explanation of the reasons why the individual or entity considers the information in question to be illegal content; (b) a clear indication of the electronic location of that information, ~~in particular~~**such as** the exact URL or URLs, and, where necessary, additional information	

MEMBER STATE	The Netherlands (hereinafter NL)	NL
GENERAL COMMENTS:		
COMMISSION PROPOSAL	Drafting suggestions	Comments
(c) the name and an electronic mail address of the individual or entity submitting the notice, except in the case of information considered to involve one of the offences referred to in Articles 3 to 7 of Directive 2011/93/EU; (d) a statement confirming the good faith belief of the individual or entity submitting the notice that the information and allegations contained therein are accurate and complete. 3. Notices ~~that include the elements~~ referred to in paragraph 2 **on the basis of which a diligent provider of hosting services can identify**	enabling the identification of the illegal content; (c) ***if necessary, in order to assess the legality of the content in question,*** the name and an electronic mail address of the individual or entity submitting the notice, except in the case of information considered to involve one of the offences referred to in Articles 3 to 7 of Directive 2011/93/EU; (d) a statement confirming the good faith belief of the individual or entity submitting the notice that the information and allegations	

MEMBER STATE	The Netherlands (hereinafter NL)	NL
GENERAL COMMENTS:		
COMMISSION PROPOSAL	Drafting suggestions	Comments
the illegality of the content in question shall be considered to give rise to actual knowledge or awareness for the purposes of Article 5 in respect of the specific item of information concerned. 4. Where the notice contains ~~the name and~~ an electronic **contact information** ~~mail address~~ of the individual or entity that submitted it, the provider of hosting services shall**,** ~~promptly~~ **without undue delay,** send a confirmation of receipt of the notice to that individual or entity. 5. The provider shall also, without undue delay, notify that individual or entity of its decision in respect of the information to which the notice	contained therein are accurate and complete. 3. Notices ~~that include the elements~~ referred to in paragraph 2 **on the basis of which a diligent provider of hosting services can identify the illegality of the content in question** shall be considered to give rise to actual knowledge or awareness for the purposes of Article 5 in respect of the specific item of information concerned. 4. Where the notice contains ~~the name and~~ an electronic **contact information** ~~mail address~~ of the individual or entity that submitted it, the provider of hosting services shall**,** ~~promptly~~ **without undue delay,** send a confirmation of	

MEMBER STATE	The Netherlands (hereinafter NL)	NL
GENERAL COMMENTS:		
COMMISSION PROPOSAL	Drafting suggestions	Comments
relates, providing information on the redress possibilities in respect of that decision. 6. Providers of hosting services shall process any notices that they receive under the mechanisms referred to in paragraph 1, and take their decisions in respect of the information to which the notices relate, in a timely, diligent and objective manner. Where they use automated means for that processing or decision-making, they shall include information on such use in the notification referred to in paragraph **5**4.	receipt of the notice to that individual or entity. 5. The provider shall also, without undue delay, notify that individual or entity of its decision in respect of the information to which the notice relates, providing information on the redress possibilities in respect of that decision ***and a clear and specific statement of reasons for that decision.*** 6. Providers of hosting services shall process any notices that they receive under the mechanisms referred to in paragraph 1, and take their decisions in respect of the information to which the notices relate, in a timely, diligent and objective manner. Where they use	

MEMBER STATE	The Netherlands (hereinafter NL)	NL
GENERAL COMMENTS:		
COMMISSION PROPOSAL	Drafting suggestions	Comments
	automated means for that processing or decision-making, they shall include information on such use in the notification referred to in paragraph **5**4.	
VLOPs		

Article 35 *Codes of conduct*	*Article 35* *Codes of conduct*	*NL thinks it is important that VLOPs participate in codes of conduct to address systemic risks and also some forms of harmful content. As example is the code of practice on disinformation that is currently being revised. Stronger language is therefore needed in this paragraph. However, we understand that participation is not legally obliged, as the VLOPs can also take other measures to mitigate systemic risks.*
1. The Commission and the Board shall encourage and facilitate the drawing up of codes of conduct at Union level to contribute to the proper application of this Regulation, taking into account in particular the specific challenges of tackling different types of illegal content and systemic risks, in accordance with Union law, in particular on competition and the protection of personal data.	1. The Commission and the Board shall encourage and facilitate the drawing up of codes of conduct at Union level to contribute to the proper application of this Regulation, taking into account in particular the specific challenges of tackling different types of illegal content and systemic risks, in accordance with Union law, in particular on competition and the protection of personal data.	
2. Where significant systemic risk within the meaning of Article 26(1) emerge and concern several very large online platforms, the Commission may invite the **providers of the** very large online platforms concerned, other	2. Where significant systemic risk within the meaning of Article 26(1) emerge and concern several very large online platforms, the Commission ***shall strongly request*** ~~***may invite***~~ the **providers of the** very large online platforms	

MEMBER STATE	The Netherlands (hereinafter NL)	NL
GENERAL COMMENTS:		
COMMISSION PROPOSAL	Drafting suggestions	Comments
providers of very large online platforms, ~~other~~ **of** online platforms and ~~other providers~~ of intermediary services, as appropriate, as well as civil society organisations and other interested parties, to participate in the drawing up of codes of conduct, including by setting out commitments to take specific risk mitigation measures, as well as a regular reporting framework on any measures taken and their outcomes.	concerned, other **providers of** very large online platforms, ~~other~~ **of** online platforms and ~~other providers~~ of intermediary services, as appropriate, as well as civil society organisations and other interested parties, to participate in the drawing up of codes of conduct, including by setting out commitments to take specific risk mitigation measures, as well as a regular reporting framework on any measures taken and their outcomes.	
3. When giving effect to paragraphs 1 and 2, the Commission and the Board shall aim to ensure that the codes of conduct clearly set out their objectives, contain key performance indicators to measure the achievement of those objectives and take due account of the needs	3. When giving effect to paragraphs 1 and 2, the Commission and the Board shall aim to ensure that the codes of conduct clearly set out their objectives, contain key performance indicators to measure the achievement of those objectives	

MEMBER STATE	The Netherlands (hereinafter NL)	NL
GENERAL COMMENTS:		
COMMISSION PROPOSAL	Drafting suggestions	Comments
and interests of all interested parties, including citizens, at Union level. The Commission and the Board shall also aim to ensure that participants report regularly to the Commission and their respective Digital Service Coordinators of establishment on any measures taken and their outcomes, as measured against the key performance indicators that they contain. 4. The Commission and the Board shall assess whether the codes of conduct meet the aims specified in paragraphs 1 and 3, and shall regularly monitor and evaluate the achievement of their objectives.	and take due account of the needs and interests of all interested parties, including citizens, at Union level. The Commission and the Board shall also aim to ensure that participants report regularly to the Commission and their respective Digital Service Coordinators of establishment on any measures taken and their outcomes, as measured against the key performance indicators that they contain. 4. The Commission and the Board shall assess whether the codes of conduct meet the aims specified in paragraphs 1 and 3, and shall regularly monitor and evaluate the achievement of their objectives.	

MEMBER STATE	The Netherlands (hereinafter NL)	NL
GENERAL COMMENTS:		
COMMISSION PROPOSAL	**Drafting suggestions**	**Comments**
They shall publish their conclusions. 5. The Board shall regularly monitor and evaluate the achievement of the objectives of the codes of conduct, having regard to the key performance indicators that they may contain.	They shall publish their conclusions. 5. The Board shall regularly monitor and evaluate the achievement of the objectives of the codes of conduct, having regard to the key performance indicators that they may contain.	
DATE OF APPLICATION		
Article 74 *Entry into force and application*		*NL believes sufficient time is required for the Member States to implement the various provisions contained in the Digital Services Act.*
1. This Regulation shall enter into force on the twentieth day following that of its publication in the *Official Journal of the European Union*.		

MEMBER STATE	The Netherlands (hereinafter NL)	NL
GENERAL COMMENTS:		
COMMISSION PROPOSAL	**Drafting suggestions**	**Comments**
2. It shall apply from [date - ~~three~~ **twelve** months after its entry into force].	2. It shall apply from [date - ~~three~~ ***~~twelve~~ eighteen*** months after its entry into force].	
This Regulation shall be binding in its entirety and directly applicable in all Member States.		
Done at Brussels,		
For the European Parliament *For the Council*		
The President The President		